AO 106 (Rev. 06/09) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Northern District of Oklahoma

In the Matter of the Search of
A WHITE 1999 SATURN SL1, OKLAHOMA LICENSE PLATE GWD 373 LOCATED OUTSIDE OF 7445 EAST 49TH STREET, APARTMENT 8-118, TULSA, OKLAHOMA, 74145, WHICH IS MORE PARTICULARY DESCRIBED IN ATTACHMENT A

Case No. 20-MJ-389-JFJ

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment "A"

located in the Northern District of Oklahoma, there is now concealed *(identify the person or describe the property to be seized):*

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC § 2261A	**Cyberstalking**

The application is based on these facts:

See Affidavit of CHRISTOPHER MCCARTHY, attached hereto.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of ___ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Christopher McCarthy
Applicant's signature

SA Christopher McCarthy, FBI
Printed name and title

Sworn to before me and signed ~~in my presence~~ by phone. JJF

Date: 10-29-20

Jodi Jayne
Judge's signature

City and state: Tulsa, OK

Jodi F. Jayne, U.S. Magistrate
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OKLAHOMA

IN THE MATTER OF THE SEARCH OF: **A WHITE 1999 SATURN SL1, OKLAHOMA LICENSE PLATE GWD 373 LOCATED OUTSIDE OF 7445 EAST 49TH STREET, APARTMENT 8-118, TULSA, OKLAHOMA, 74145, WHICH IS MORE PARTICULARY DESCRIBED IN ATTACHMENT A**	Case No.

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Christopher McCarthy, a Special Agent (SA) with the Federal Bureau of Investigation (FBI), being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as **A WHITE 1999 SATURN SL1, OKLAHOMA LICENSE PLATE GWD 373,** hereinafter "PREMISES," further described in Attachment A, for the things described in Attachment B.

2. As a Federal Law Enforcement Officer, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States. I am a Special Agent with the FBI and have been since November 2019. I am currently assigned to the Tulsa Resident Agency of the Oklahoma City Division. Since joining the FBI, I have

investigated violation of federal law. I have gained experience through training in classes and work related to conducting these types of investigations.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. The information contained in this affidavit is based upon:

- my personal knowledge and observation;
- my training and experience;
- conversations with other law enforcement officers and witnesses and;
- review and analysis of documents and records.

5. I request a warrant to search the PREMISES for the items specified in Attachment B hereto, which constitute instrumentalities, fruits, and evidence of violations of 18 U.S.C. § 2261A (Cyberstalking). The term "SUBJECT PREMISES" is meant to encompass the following, to the extent they are located at/on the property known as **A 1999 WHITE SATURN SL1, OKLAHOMA LICENSE PLATE GWD 373 LOCATED OUTSIDE OF 7445 EAST 49TH STREET, APARTMENT 8-118, TULSA, OKLAHOMA, 74145:**

a. the containers, persons, and property such as a computer (as broadly defined in 18 U.S.C. § 1030(e)(1)) or other digital file storage device located there.

6. This investigation, described more fully below, has revealed that an individual knowingly utilized a computer from 7445 East 49th Street, Apartment 8-118, Tulsa, Oklahoma, 74145 to violate the foregoing statute. There is probable cause to believe that evidence, fruits, and instrumentalities of such violations are located at the PREMISES, which is parked in close vicinity to the apartment described above and used by Jeffries immediately prior to his arrest.

7. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me regarding this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to support the issuance of a search warrant.

PROBABLE CAUSE

8. Your affiant describes the subject of this investigation as Brannon Jeffries, date of birth 11/22/1985, black male, residing in or around Tulsa, OK.

9. Victim 1 and BRANNON JEFFRIES began a romantic relationship in or around November 2018 after connecting online. Victim 1 lived in Kansas. In January 2019, Victim 1 became aware of JEFFRIES' criminal history and terminated the relationship. In approximately March 2019, a friend of JEFFRIES' informed Victim 1 that JEFFRIES planned to acquire a firearm and travel to Kansas to see her. Around this time, JEFFRIES created Facebook and Twitter pages in Victim 1's name and likeness. JEFFRIES posted intimate photos on the pages

and attempted to "friend" Victim 1's sister while sharing the photos. JEFFRIES also attempted to repeatedly call Victim 1 from the imposter accounts. Victim 1 reported the situation to the Olathe Police Department, Kansas.

10. Throughout the end of March and beginning of April 2019, Victim 1 re-opened communication with JEFFRIES in an attempt to be civil and de-escalate the situation. Throughout a series of recorded phone calls that Victim 1 provided to the FBI, JEFFRIES acknowledged creating the pages and the threat of gun violence. Furthermore, he expressed that he "couldn't *not* be mad" (emphasis added) every day he was not with Victim 1. He explained his actions as retaliation on Victim 1 for hurting him [by breaking up with him] and needing to hurt her equally through imposter social media accounts, humiliation, and the threat of violence. On April 7, 2019, JEFFRIES stated that only "revenge" could bring him peace. Throughout the phone calls, Victim 1 expressed to JEFFRIES her distress at his actions. On at least one occasion, she could be heard crying, and JEFFRIES told her to stop.

11. Victim 1 cut off communication for good in May 2019, and she changed her phone number. When JEFFRIES made new imposter accounts, Victim 1 reported them to Facebook and Twitter to have them removed. Victim 1 continued to receive calls from Google Voice or Facebook, and she ignored what she believed to be entreaties from JEFFRIES. In large part to move farther from JEFFRIES, Victim 1 moved to Savannah, Georgia, in or around April 2020.

12. On or around August 31, 2020, Victim 1 received a letter through the United States Postal Service at her apartment in Savannah. Her type-written name, nickname, and address were taped onto the front of the envelope, which was postmarked Tulsa, OK, with no return address. The envelope was taped closed. Inside the envelope was a single page note with the word "Inevitable" typed on the page. New imposter social media accounts contacted Victim 1 at this time. Victim 1 reported the incidents to the Savannah Police Department on September 9, 2020.

13. On October 12, 2020, Victim 1 googled her own name and discovered that a website had been created using her full name as the domain. This site was created with and hosted by GoDaddy on September 25, 2020. The website purported to be Victim 1, stating she was "very interested in being gangbanged," criticizing and sexualizing her mother, and disparaging Victim 1's loyalty and character. The site featured screenshots of at least one imposter Twitter account and had a gallery of intimate and nude photographs of Victim 1. In one photo, a black male stands behind Victim 1, holding her breasts. His face is marked out of the photo, however, Victim 1 identified the male as Jeffries.

14. On October 13, 2020, Victim 1 reported the aforementioned events to the FBI.

15. On October 19, 2020, Victim 1 received an email from BRANDIINFIELDS@GMAIL.COM, an email address theretofore unknown to Victim 1, claiming to have come across the website and inquiring if Victim 1 was "aware of the content on

there." Less than one and a half hours after the email, Victim 1 missed a call from an imposter Facebook account (Victim 1's name).

16. On October 15 and 16, 2020, preservation letters were served on GoDaddy, Facebook, and Twitter. On October 19, 2020, federal grand jury subpoenas for the accounts in question were served on these three companies. On October 19, 2020, a preservation letter was served on Google for BRANDIINFIELDS@GMAIL.COM. The letter sent to Victim 1 in August 2020 is pending fingerprint analysis at the FBI Lab.

17. Results of the aforementioned legal processes are pending as of October 27, 2020.

18. On October 27, 2020, in the presence of FBI SA Savannah Solomon, agent with the FBI working in Georgia, Victim 1 used the Facebook messenger application to call the Facebook user (Victim 1's name) that attempted to call Victim 1 on and before October 19, 2020. The initial call attempt did not connect, so Victim 1 text messaged the user "Brannon we need to talk." Within minutes, the user responded, "You can call me." Victim 1 called the account and addressed the user as "Brannon." Victim 1 asked Jeffries when "all of this" was going to stop. Throughout the 3 minute 48 second call, Jeffries stated he was "angry" that Victim 1 had changed her phone number after they last spoke. Jeffries stated this action was disrespectful to him. Victim 1 addressed the imposter social media accounts and "the website." She asked if Jeffries knew what putting "all that out there" could do to her. When she asked Jeffries how long this would all go on, he responded with silence. When asked again, he said

"what you think?" Victim 1 said she assumed now it would last forever. The call ended when Jeffries said he needed to return to work, but he insisted Victim 1 call him later in the afternoon to continue the conversation. SA Solomon observed Victim 1 shaking while she spoke to JEFFRIES, and she cried following the interaction. SA Solomon attempted to record the phone call; however, it was discovered after the fact that the recording device malfunctioned.

19. During her reports to the FBI, Victim 1 has expressed distress and disbelief that the harassment has continued for almost two years. During each in person interaction with Victim 1, SA Solomon observed Victim 1 come to tears. Victim 1 has expressed fear of retaliation from JEFFRIES, concern for her own safety and that of her family, and the impact of JEFFRIES' actions on her professional career.

20. Jeffries has a current state warrant for his arrest out of Wisconsin for "online harassment." Jeffries was convicted on felony sex crimes in or around 2010. The initial police report from Memphis, TN, identified Jeffries as a subject that had raped two women at gunpoint. As a result, Jeffries is required to register as a sexual offender. In March of 2011, he pleaded guilty to federal charges under 18 U.S.C. § 2250(a) after failing to register as a sex offender.

21. Your affiant conducted a records check via Accurint, a locate-and-research tool available to law enforcement run by LexisNexis. The Accurint records indicated that Jeffries had resided at the 7445 East 49th Street, Apartment 8-118, Tulsa, Oklahoma, 74145 since April 2017. Your affiant reviewed an appearance bond filed in Jeffries' state case for failing to

register as a sex offender (Tulsa County CF-2020-2133). The appearance bond paperwork filed on the Oklahoma State Court Network website under his case number shows the 7445 East 49th Street, Apartment 8-118, Tulsa, Oklahoma, 74145 as his address. Your affiant also conducted surveillance on October 20, 2020 and observed Jeffries leaving the building containing the 7445 East 49th Street, Apartment 8-118, Tulsa, Oklahoma, 74145, entering a 1999 Saturn SL1, Oklahoma License Plate GWD 373 registered to his father, and departing.

22. On the morning of October 29, 2020, your affiant and a team with the FBI executed a federal search warrant signed in the Northern District of Oklahoma on October 28, 2020 for 7445 East 49th Street, Apartment 8-118, Tulsa, Oklahoma, 74145. Jeffries was not present at the apartment. One laptop was found.

23. At the FBI's request, the apartment's leasing office arranged for Jeffries to return to the apartment. At approximately 10:45 AM, Jeffries returned in the 1999 Saturn SL1, Oklahoma License Plate GWD 373. He parked the vehicle next to a fire hydrant. As he exited the vehicle, he was arrested. His cell phone was found on his person. Agents observed a backpack inside of the vehicle as he exited it.

24. Attachment A of the Northern District of Oklahoma warrant signed on October 28, 2020 for a search of 7445 East 49th Street, Apartment 8-118, Tulsa, Oklahoma, 74145, authorized a search of "any vehicles parked in parking spaces assigned to Apartment 8-118." Jeffries did not park the 1999 Saturn SL1, Oklahoma License Plate GWD 373. However,

officers observed Jeffries drive up in and depart the vehicle immediately before they arrested him.

25. Based on my training and experience, individuals carry portable electronic devices with them when they travel in vehicles. Frequently, they will carry more than one portable electronic device. They may also store electronic devices or phones in a vehicle that they use regularly. Here, Jeffries was leaving the vehicle he has been observed using before while in the immediate vicinity of the apartment searched pursuant to the federal warrant signed on October 28, 2020.

26. The vehicle is currently parked by the fire hydrant where Jeffries left it. It is currently under the supervision of agents pending this warrant.

TECHNICAL TERMS

27. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be

directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

28. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage

media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

29. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

30. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a

file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and

malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the subject. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs,

may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on

the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to obtain unauthorized access to a victim computer over the Internet, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

31. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

32. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

33. I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A and seize the items described in Attachment B.

Respectfully submitted,

Christopher McCarthy
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me by phone
on October 29, 2020:

UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be searched

The property to be searched is **A WHITE 1999 SATURN SL1, OKLAHOMA LICENSE PLATE GWD 373 LOCATED OUTSIDE OF 7445 EAST 49TH STREET, APARTMENT 8-118, TULSA, OKLAHOMA, 74145.**

ATTACHMENT B

Property to be seized

1. All records relating to violations of 18 USC § 2261A (Cyberstalking) from November 2018 to the present day, including:

   a. Records and information relating to Victim 1;

   b. Records and information relating to the e-mail account BRANDIINFIELDS@GMAIL.COM;

   c. Records and information relating to the identity or location of the subjects;

   d. Records and information relating to malicious software and computer or email account intrusion;

2. Computers or storage media used as a means to commit the violations described above.

   a. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

      i. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and

passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

ii. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the lack of such malicious software;

iv. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

v. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

vi. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

vii. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

viii. evidence of the times the COMPUTER was used;

ix. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

x. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

xi. records of or information about Internet Protocol addresses used by the COMPUTER;

xii. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

xiii. contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.